



# **Need-Based Network Traffic Collection**

**Nathan Dell and Angela Horneman**

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>15 FEB 2015</b>		2. REPORT TYPE <b>N/A</b>		3. DATES COVERED	
4. TITLE AND SUBTITLE <b>Need Based Network Traffic Collection</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) <b>Horneman /Angela</b>				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release, distribution unlimited.</b>					
13. SUPPLEMENTARY NOTES <b>The original document contains color images.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>SAR</b>	18. NUMBER OF PAGES <b>14</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

---

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

DM-0002061

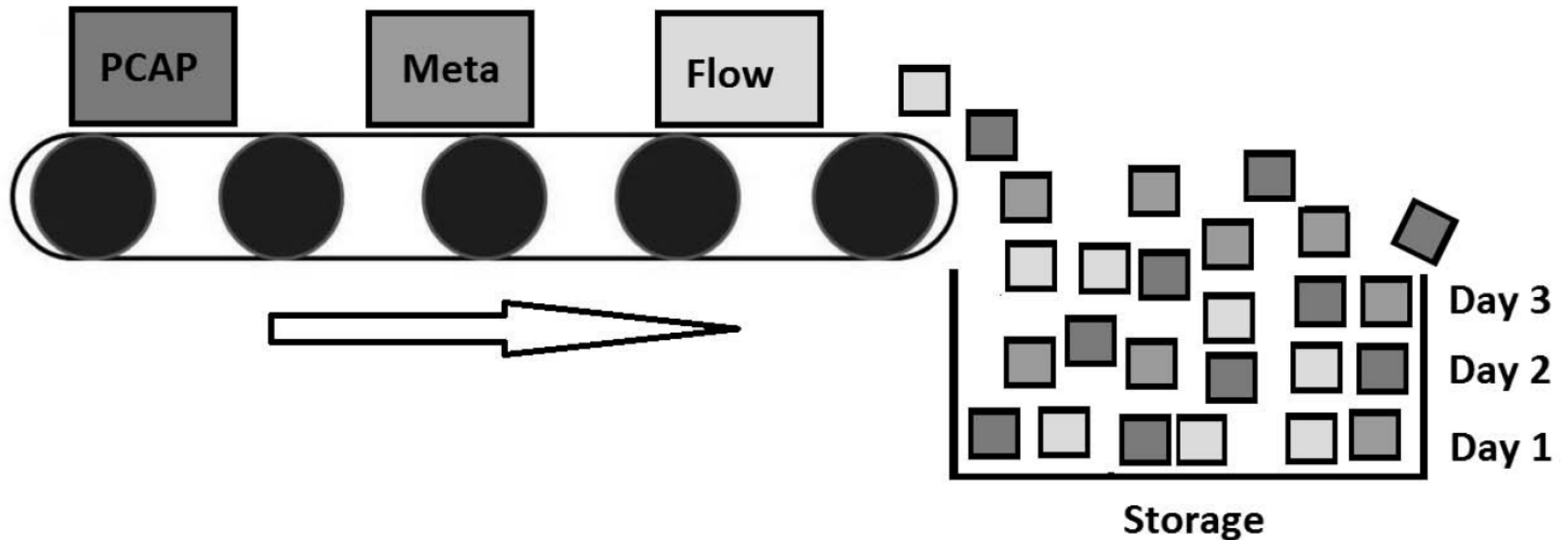
# Background

---

Network traffic monitoring is important.

Storage is important.

Analysis is important.



# The Problem

---

“Collect everything mentality” is not effective.

- Network data typically rolls off before it becomes useful to analysts
- Some data collected has little to no value ever.
- Too much data inhibits analysis.
- Storage can become expensive.

When you can't keep everything, what do you do?

# The Solution

---

A methodology to help organizations to collect

- the right network information
- at the right tiers
- for the right amount of time

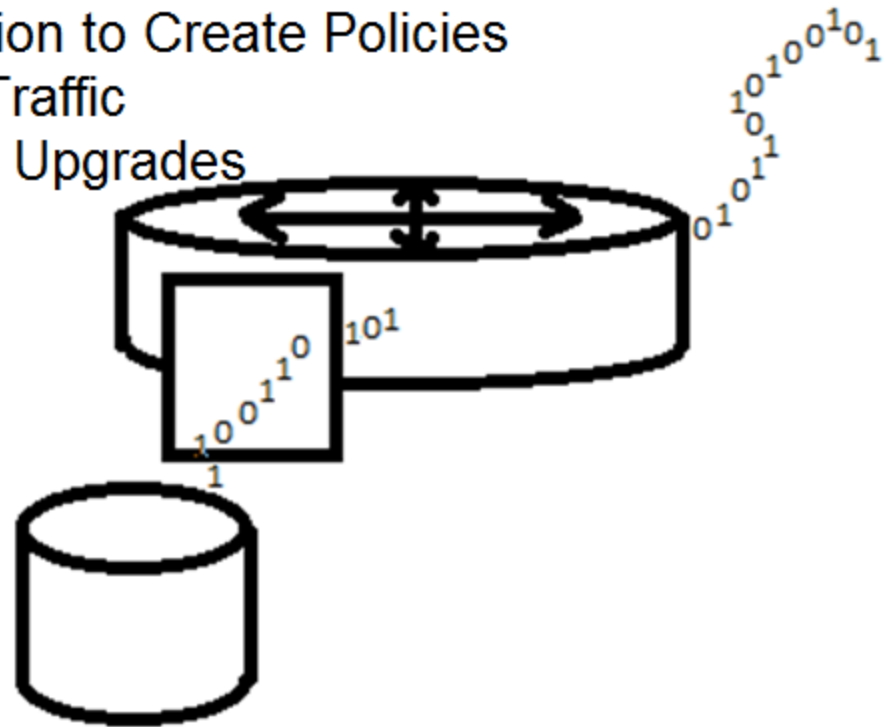
## Smart Collection and Storage Method for Network Traffic Data

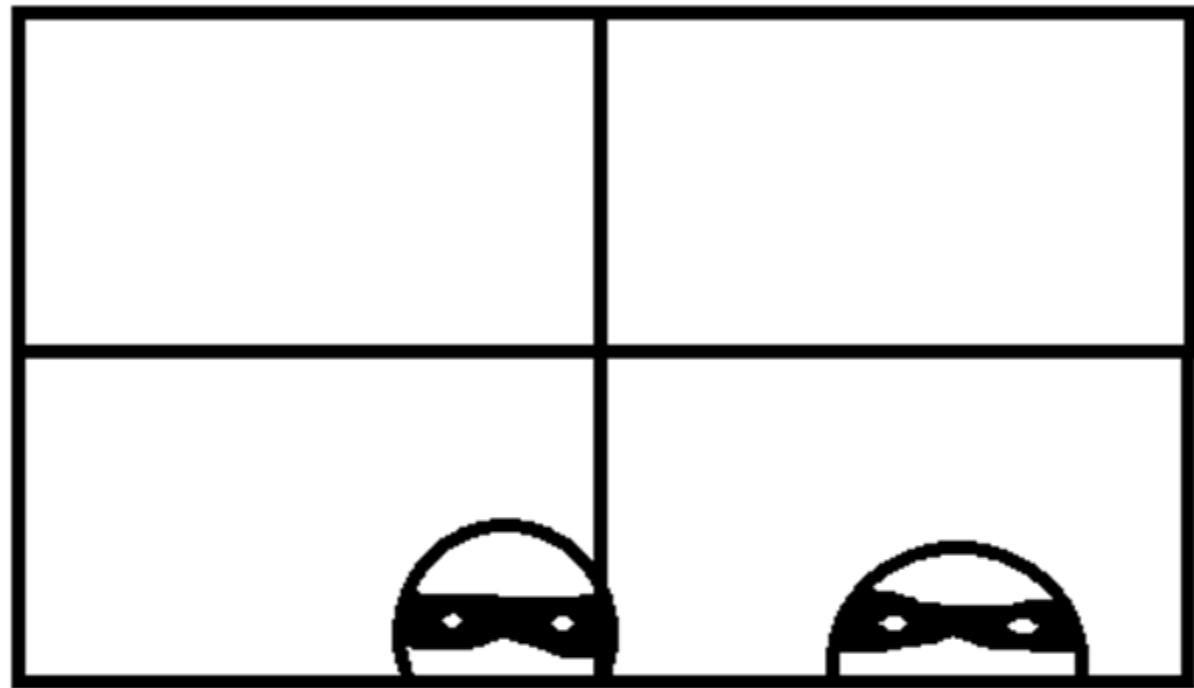
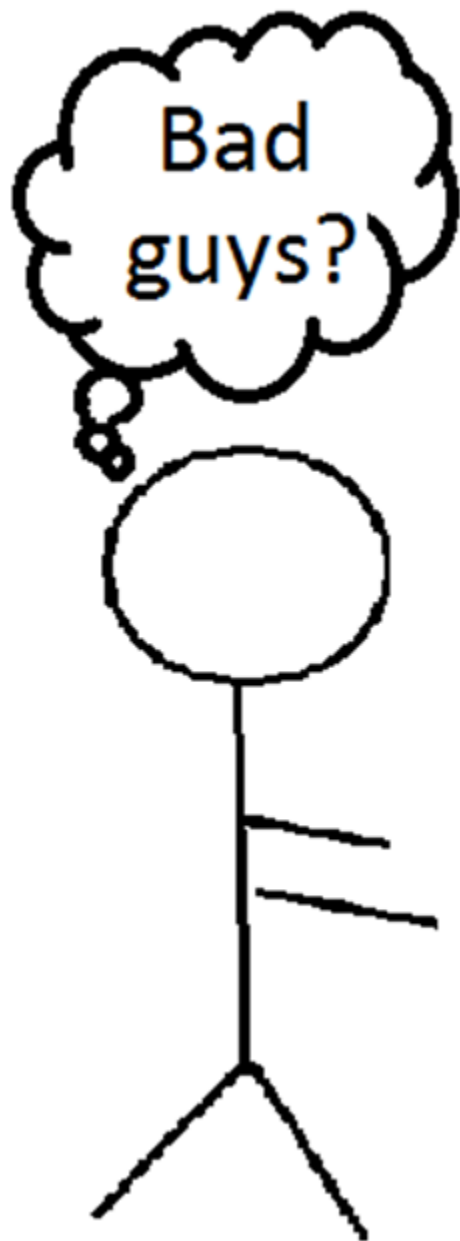
Available online in the SEI Digital Library

<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=304860>

Why do I need this?

- ✓ Investigate Attacks
- ✓ Enforce Policies
- ✓ Provide Information to Create Policies
- ✓ Profile Network Traffic
- ✓ Plan for Network Upgrades

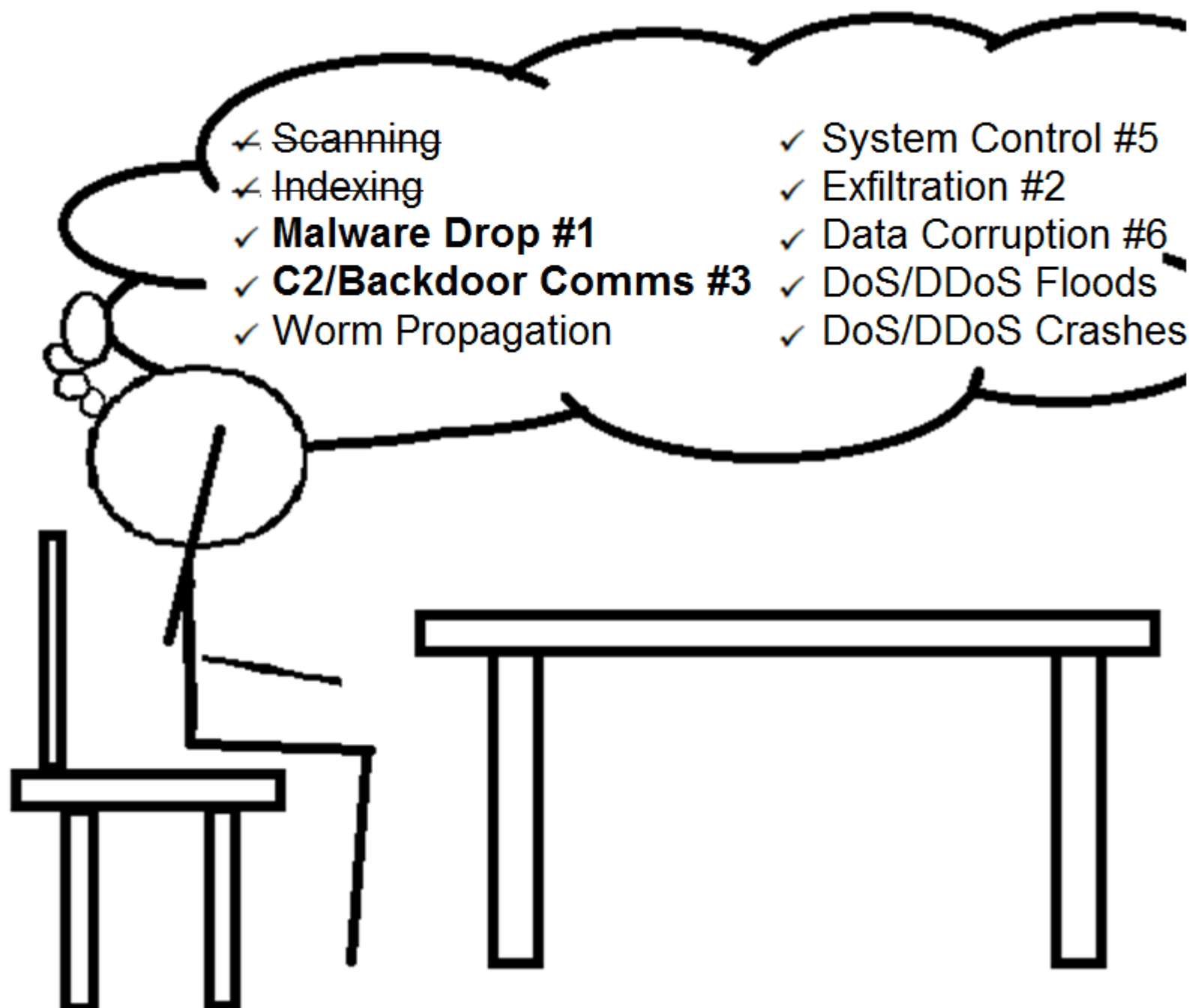


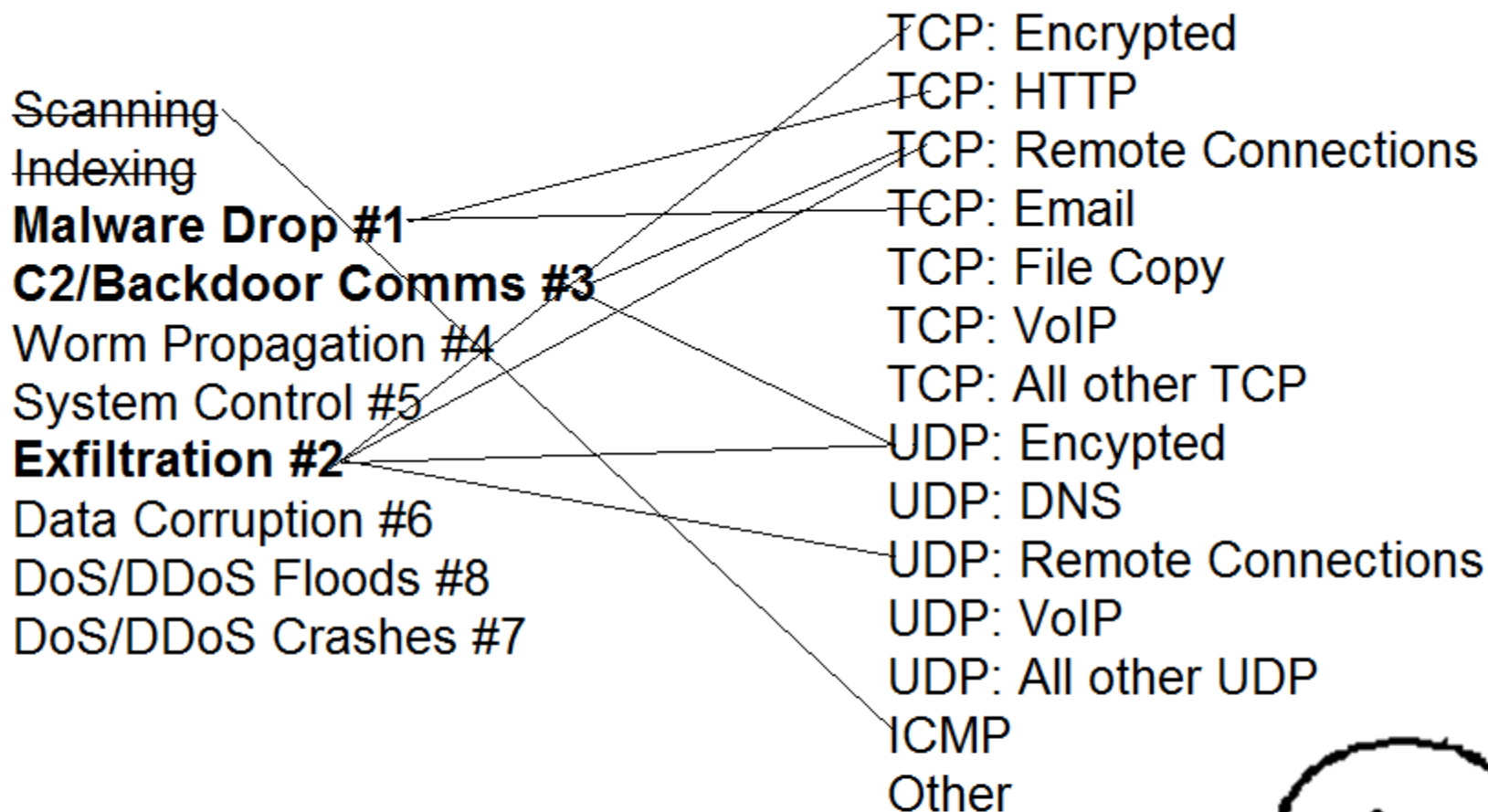


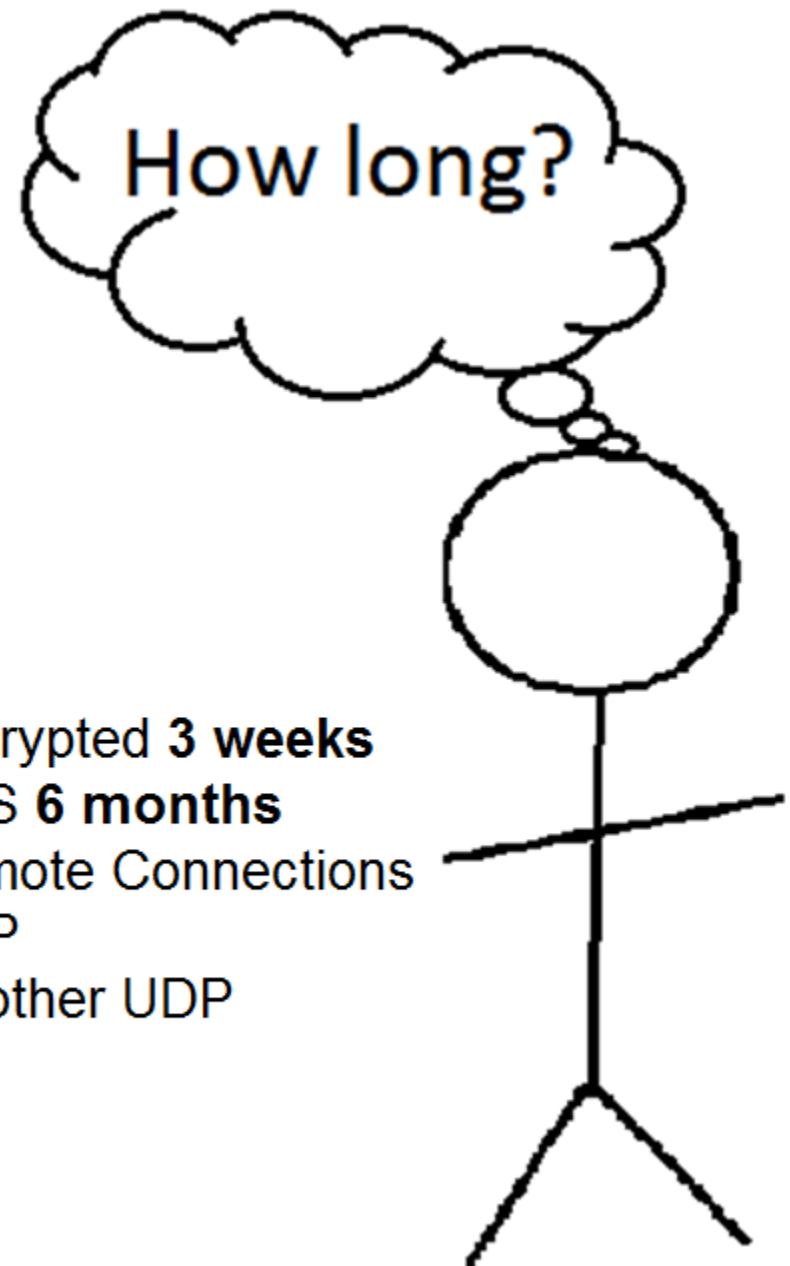
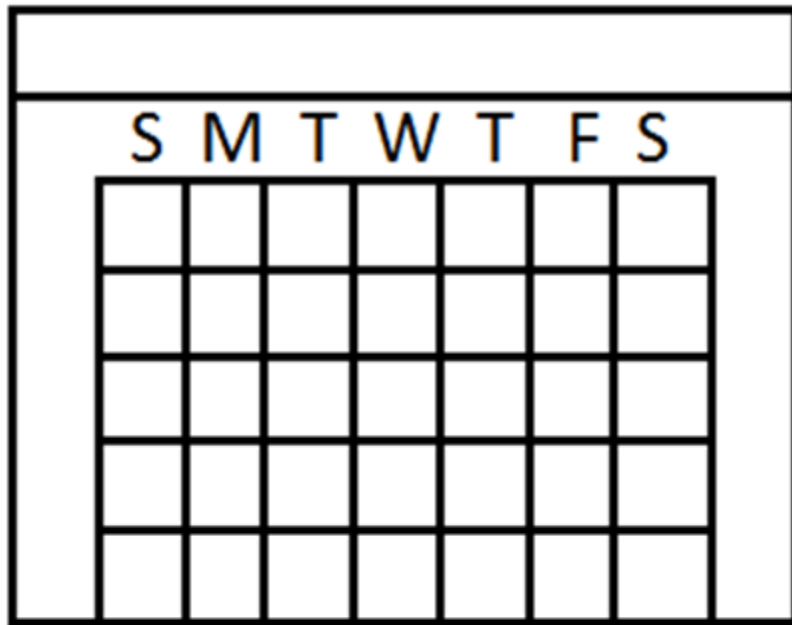
- ✓ Scanning
- ✓ Indexing
- ✓ Malware Drop
- ✓ C2/Backdoor Comms
- ✓ Worm Propagation

- ✓ System Control
- ✓ Exfiltration
- ✓ Data Corruption
- ✓ DoS/DDoS Floods
- ✓ DoS/DDoS Crashes









TCP: Encrypted **3 weeks**

TCP: HTTP **6 months**

TCP: Remote Connections

TCP: Email **2 years**

TCP: File Copy

TCP: VoIP

TCP: All other TCP

UDP: Encrypted **3 weeks**

UDP: DNS **6 months**

UDP: Remote Connections

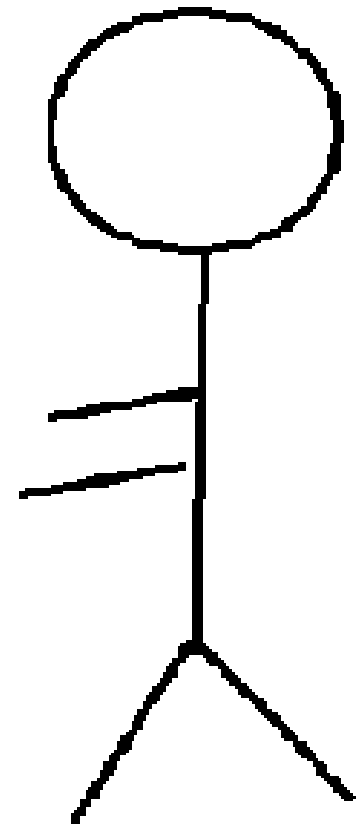
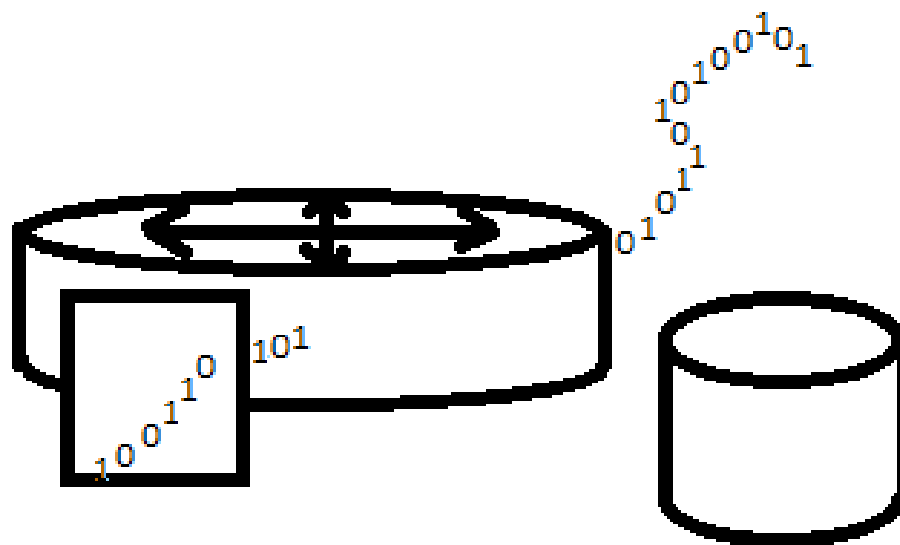
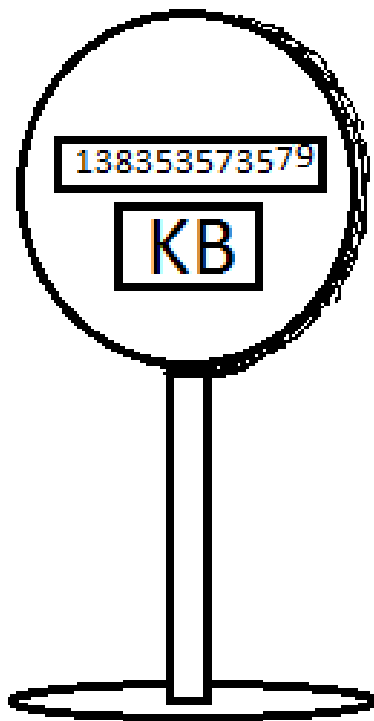
UDP: VoIP

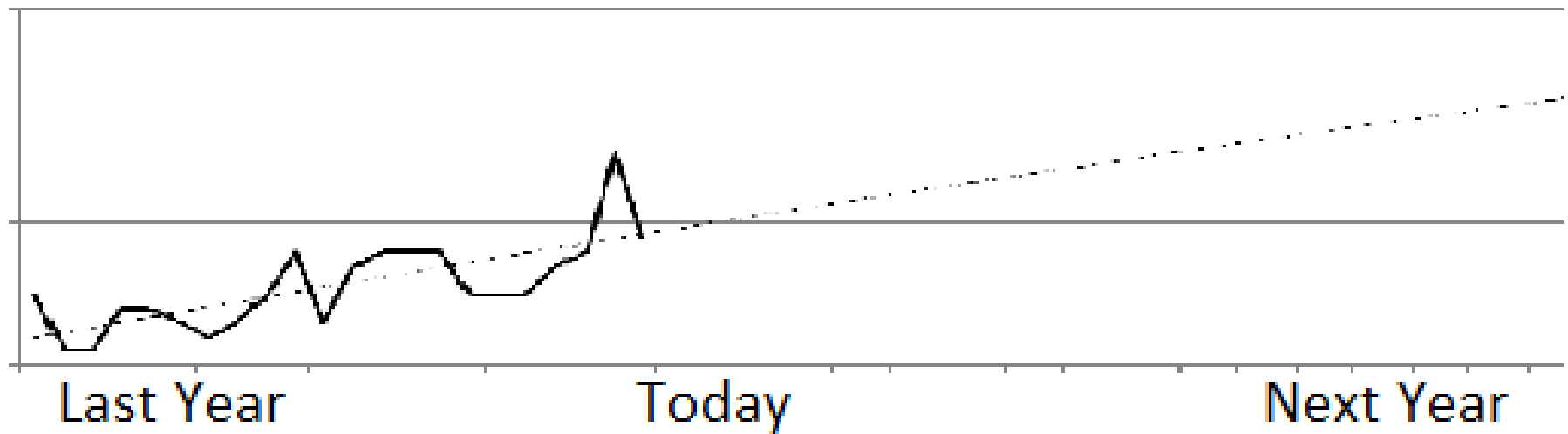
UDP: All other UDP

ICMP

Other

How much  
storage?





# Application of the Methodology

$$\text{Current Storage X } (1 + \text{Growth Rate})^{\text{Months}} \left( \frac{\text{ending value}}{\text{starting value}} \right)^{\left( \frac{1}{\# \text{ months}} \right)} - 1$$

	Monthly Growth Rates				Storage per Day in 24 Months: All			Storage per Day in 24 Months: Peak		
	All Traffic (Bytes)	Peak Traffic (Bytes)	All Traffic (Flows)	Peak Traffic (Flows)	N (in GBs)	A (in GBs)	P (in TBs)	N (in GBs)	A (in GBs)	P (in TBs)
<b>TCP: HTTP</b>	0.92%	2.47%	0.92%	2.47%	292.7	443.3	223.9	351.4	532.3	268.9
<b>TCP: Encrypted HTTP</b>	0.92%	2.47%	0.92%	2.47%	154.0	<b>233.3</b>	<b>128.1</b>	184.9	<b>280.2</b>	<b>153.9</b>
<b>TCP: VoIP</b>	0.61%	3.41%	0.61%	2.16%	0.0	0.0	<b>0.0</b>	0.0	0.1	<b>0.0</b>
<b>UDP: VoIP</b>	0.92%	2.47%	0.92%	2.47%	2.9	4.3	<b>0.0</b>	3.4	5.2	<b>0.1</b>
<b>UDP: Encrypted VoIP</b>	0.61%	1.85%	0.61%	1.85%	0.0	0.1	<b>0.0</b>	0.0	0.1	<b>0.0</b>
				Unfiltered:		<b>1225.3</b>	<b>603.1</b>		<b>1494.0</b>	<b>728.6</b>
				Filtered:	808.8	978.3	469.1	982.3	1197.4	567.5

# Questions?

---

Angela Horneman  
[ahorneman@cert.org](mailto:ahorneman@cert.org)

Nathan Dell  
[nathand@cert.org](mailto:nathand@cert.org)